Statement of Dr. F. Thomson Leighton

Co-Founder and Chief Scientist, Akamai Technologies, Inc.,
Professor of Applied Mathematics, MIT,

Testimony before the
Committee on Science
U.S. House of Representatives

Hearing on "The Future of Computer Science Research in the U.S."

Thursday, May 12, 2005

Chairman Boehlert, Ranking Member Gordon, and Members of the Committee, I appreciate the opportunity to testify this morning about the Future of Computer Science Research in the United States.

I am appearing today in my role as the Co-founder and Chief Scientist of Akamai Technologies. I am also a Professor of Applied Mathematics at MIT, a member of the President's Information Technology Advisory Committee (PITAC), and Chair of the PITAC Subcommittee on Cyber Security.

Although I will focus my remarks on the crisis this Nation faces in the area of cyber security, the challenges we face with cyber security research are very similar to those we face with IT at large. Namely, there is much research that urgently needs to be done, little of which will be funded by industry. And, the current underinvestment in fundamental research by the Government could lead to dire consequences for the Nation.

Akamai is the leading supplier of content delivery services on the Internet. Using sophisticated algorithms to coordinate the operation of 15,000 web servers in 70 countries, Akamai distributes content and applications from thousands of Web sites to hundreds of millions of consumers worldwide. We serve each of you every day. One out of every five Global 500 companies and many Government agencies (including the House of Representatives) utilize the Akamai platform to distribute their content and applications over the Internet.

As part of our business, we provide the primary means of defense against cyber attacks for many web sites. When the FBI web site was brought down on September 11, 2001, they turned to Akamai to help them restore service. On behalf of our customers, we fight a nonstop battle against cyber attacks that are increasing in sophistication and scale every day.

Like the Internet itself, Akamai evolved from what was originally an academic research project sponsored by the Defense Advanced Research Projects Agency (DARPA). DARPA has a long and very successful history of funding research by the nation's best computer scientists. But recently, DARPA has shifted funding away from fundamental research at universities in favor of financing classified work and/or more development-related projects.

If DARPA's current practices had been in effect in the mid-1990s, it is unlikely that the development of Akamai's technology, designed to improve the distribution of content and applications over the Internet, would have taken place. That is because no other agency has stepped in to fill the gap created by the shift at DARPA. This is particularly evident in the area of cyber security.

Although the Department of Homeland Security (DHS) is tasked with providing security for the homeland, including cyber security, it spends less than 2% of its Science and Technology budget on cyber security, and, of that amount, less than 1/10 (a mere $2 million) is spent on fundamental research for cyber security.

Although many agencies are concerned with cyber security, the National Science Foundation (NSF) has the only substantial program for funding fundamental research on cyber security, and it is seriously under funded. In 2004, NSF funded just 8% of qualified research proposals in the area of cyber security. This is a factor of three less than the overall agency average. In the related area of computer science and engineering, the funding rate is only 16%, and decreasing. In fact, the success rate for NSF's Computer and Information Science and Engineering (CISE) Directorate proposals has dropped by a factor of two over the last four years.

As a result of the changes in government funding for basic research, we are now facing a serious lag in our Nation's ability to continue to innovate, and at a time when innovation is most needed.

The need for innovation is especially urgent in the area of cyber security. Because of the great improvements in functionality and efficiency afforded by Internet technology, it has been incorporated into most every aspect of our society. Today, virtually every sector of the Nation's infrastructure – including communications, utilities, finance, transportation, law enforcement, and defense -- is now critically reliant on networking technology.

Unfortunately, the revolution in connectivity afforded by the Internet has also dramatically increased the capabilities of those who would do harm. Today, it is possible for a malicious agent to penetrate millions of computers around the world in a matter of minutes, exploiting those machines to attack the Nation's critical infrastructure, penetrate sensitive systems, or steal valuable data. The growth in the number of attacks matches the tremendous growth in connectivity, and dealing with these attacks now costs the Nation billions of dollars annually. We have included numerous statistics that document the rapidly escalating nature of the cyber security problem in the PITAC report, titled "Cyber Security: A Crisis in Prioritization." I will mention just a few here.

In the last half of 2004, over 7,000 different viruses and worms were released across the Internet. This is a 64% increase over the first six months of 2004.[1] Because of such viruses and worms, the percentage of computers that became infected each month grew from 1% in 1996 to over 10% per month in 2003.[2]

These infected computers reside in our homes, offices, and schools. No computer is immune. Indeed, the networks of 40% of the Fortune 100 companies were so severely compromised in 2003 that they became the source of a spreading virus.[3]

Once infected, a computer can be reprogrammed so as to reveal confidential information to attackers, destroy or alter important data, and/or to carry out attacks against others. When infected computers are incorporated into so-called "bot armies," they can be used as platforms for launching unwanted spam or, even worse, denial of service attacks against critical infrastructure. In the first half of 2004, the rate at which newly-infected computers were incorporated into bot armies rose from 2,000 per day to over 30,000 per day.[4]

The use of bot armies to attack web sites has given rise to a new form of crime known as cyber extortion, in which the criminal will demand payment in return for not attacking a businesses' web presence. Although cyber extortion was unheard of just a few years ago, 17 out of 100 companies surveyed in a recent poll reported being the target of cyber extortion in 2004.[5]

[1] Symantec, *Internet Security Threat Report*, March 21, 2005

[2] ICSA Labs Virus Alerts; PITAC -- February 2005 Report "*Cyber Security: A Crisis of Prioritization*" p. 10

[3] Symantec *Internet Security Threat Report*, March 21, 2005

[4] PITAC -- February 2005 Report "*Cyber Security: A Crisis of Prioritization*" p. 10

[5] 2004 poll by Carnegie Mellon University-*InformationWeek;* PITAC -- February 2005 Report "*Cyber Security: A Crisis of Prioritization*" p. 8

The financial sector is one of many key industry segments that are being particularly hard hit by cyber crime. 83% of financial institutions reported compromised systems in 2003, more than double the rate in 2001. The use of Phishing scams to direct unwitting citizens to fake web sites, whereupon they are tricked into revealing their passwords and other sensitive information is now rampant.[6]

In the last two months, a new and even more pernicious kind of attack known as Pharming has become widespread.[7] Pharming is different from phishing in that it makes use of fundamental vulnerabilities in the basic protocols that are used to run the Internet. As a result, the attack is virtually undetectable, even by an experienced professional.

It is estimated that over 1% of US households fell victim to electronic identity theft at a cost of over $400M in the first six months of 2004.[8] Everyone is vulnerable. Today, a criminal can steal almost any password that is used for access over the Internet.

Beyond the economic repercussions, there are serious risks to our national security. Today, virtually every sector of the Nation's infrastructure – including communications, utilities, finance, transportation, law enforcement, and defense -- is critically reliant on networked IT systems, and these systems have very little, if any, defense against cyber attack.

All elements of the Nation's infrastructure are insecure if IT is insecure, and, today, our IT is insecure.

Our national defense systems are also at risk, because the military increasingly relies on many of the same vulnerable IT systems as the civilian sector. This is one reason why it is vital that DARPA not ignore the civilian sector when allocating funds for cyber security research.

[6] Anti-Phishing Working Group (www.antiphishing.org)

[7] Anti-Phishing Working Group (www.antiphishing.org)

[8] Consumers Union (www.consumersunion.org); PITAC -- February 2005 Report "*Cyber Security: A Crisis of Prioritization*" p. 9

In response to the growing crisis, some have stated that if only the citizens at home and in small business would keep their firewalls and software patches up to date, we would be OK. While such safeguards are clearly necessary, they are far from sufficient. After all, if the most sophisticated and IT-savvy companies in the world are routinely falling victim to cyber attacks, how can we expect our citizens at home and in small business to fare any better?

Moreover, the problem is not just about ubiquitous software that is vulnerable to viruses and worms. The core protocols that form the underpinnings of the Internet were simply not designed with security in mind.

We are now just beginning to see the effects of a decades-long failure to develop the security protocols and practices needed to protect the Nation's IT infrastructure, and to adequately train and grow the numbers of experts needed to employ those mechanisms effectively. The short term patches and fixes that are deployed today can be useful in response to isolated vulnerabilities, but they do not adequately address the core problems.

In order to make true progress against the core problems that plague our IT infrastructure, PITAC has stated its belief that fundamental research is required to develop entirely new approaches to cyber security. It recommends that the NSF budget for cyber security be increased by $90M annually and that DARPA restore its historical role of funding basic, unclassified research in cyber security. PITAC also recommends that DHS significantly expand its funding for cyber security research.

The report goes on to describe ten specific research areas that are in the greatest need of support as well as specific recommendations to improve coordination of research efforts, to facilitate technology transfer, and to increase the pool of experienced researchers in the area of cyber security.

In summary, the PITAC finds that the IT infrastructure of the United States -- and thus all other elements of our infrastructure that rely on IT, such as the electric power system, the government, and the military -- is highly vulnerable to terrorist and criminal attacks. Fundamental research is urgently required to improve our defenses. It is imperative that the Federal Government take action before the situation worsens and the cost of inaction becomes even greater.

Thank you.

Appendices to Testimony before The Committee on Science

U.S. House of Representatives

Thursday, May 12, 2005

Appendix A

The Threat from “Phishing” and “Pharming”

(excerpts from: *The Arizona Republic* **–** 'Pharmers' hit online bank users with fraud scam**,** April 22, 2005, by Jane Larson)

A new malicious cyber security crime is emerging that has serious ramifications for consumers, business, and even government agencies. The criminal act is called pharming — a play on "phishing," and another type of Internet fraud — that involves highly skilled hackers who secretly redirect users' computers from financial sites to the scammers' fake ones, where they steal passwords and other personal information. Even the Web address looks the same.

Unlike phishing, where users click on links in e-mails and are taken to fake sites, pharming intercepts a user on his or her way to the bank or credit-card firm. And it potentially can affect thousands of users at a time. Hackers are targeting small sections of the Internet and rerouting traffic to fake bank sites to capture users' passwords. The legitimate sites don't notice the drop in Web traffic because it is just a fraction of the total.

Criminals can 'pharm' data online with little or no knowledge by consumers. Even experienced Internet users can become victims and not know it. It is just a matter of time before the scam becomes widespread.

An anti-phishing bill introduced in Congress last month would also apply to pharming. It calls for prison time and fines for those caught either phishing or pharming.

Consider the following facts:

- Over 7,300 new Windows-based virus and worm variants emerged over the last six months of 2004. This is a 64% increase over the first six months of 2004. (Symantec)

- Over 2,600 active phishing sites were reported in February of 2005 (Anti-Phishing Working Group)

- 64 brand name businesses were targeted by phishing scams in January 2005. (Anti-Phishing Working Group)

- The United States ranks first among countries hosting the most phishing Web sites (Anti-Phishing Working Group)

Pharmers have four main ways of operating: attacking a user’s computer, attacking the large servers that find Web sites for users, compromising the routing infrastructure, or by intercepting wireless communications.

The first way is to send virus-laden e-mails that install small software programs on users' computers. When a user tries to go to his bank's Web site, the program redirects the browser to the pharmers' fake site. It then asks a user to update information such as log ons, PIN codes or driver's license numbers. Scammers use the information to steal identities.

Other viruses, called key loggers, track a user's key strokes on legitimate sites and can be used to steal passwords.

The pharmers' second method takes advantage of the fact that Web sites have verbal names but reside at numeric addresses on the Internet. When users type a Web site's name into their browsers, Domain Name System (DNS) servers read the name and look up its numeric address so that users can get to the site.

Pharmers interfere with that process by changing the real site's numeric address to the fake site's numeric address.

The servers can belong to financial institutions, Web-hosting companies or Internet service providers. This tactic, called DNS poisoning, has been around for years, but it is only in the past six months that techies have seen it used for identity theft and dubbed it pharming.

The third way is by sending incorrect data to an Internet router, exploiting the fact that the Border Gateway Protocol (BGP) has no security. A hacker can then induce the router to send traffic to the wrong place.

The fourth method is to intercept wireless traffic. If a user is, for example, in a cyber/wireless café, a hacker can bring his own Dynamic Host Configuration Protocol (DHCP) server, intercept a wireless signal, and reply to an end user’s Internet request prior to the response from the actual origin page. The hacker then takes over the session, and is controlling all communications.

What is alarming is that pharming can reroute many thousands of Internet users at a time, making the impact potentially huge. With phishing, you're scamming one person at a time; pharming allows you to scam a large group at once.

Pharming can also easily be evolved to impact businesses and military personnel, essentially collecting confidential data, and jeopardizing national infrastructure.

Appendix B

PITAC Letter to the President

February 28, 2005
The Honorable George W. Bush
President of the United States
The White House
Washington, D.C. 20500

Dear Mr. President:

We submit to you the enclosed report entitled *Cyber Security: A Crisis of Prioritization.* For nearly a year, the President's Information Technology Advisory Committee (PITAC) has studied the security of the information technology (IT) infrastructure of the United States, which is essential to national and homeland security as well as everyday life.

The IT infrastructure is highly vulnerable to premeditated attacks with potentially catastrophic effects. Thus, it is a prime target for cyber terrorism as well as criminal acts. The IT infrastructure encompasses not only the best-known uses of the public Internet – e-commerce, communication, and Web services – but also the less visible systems and connections of the Nation's critical infrastructures such as power grids, air traffic control systems, financial systems, and military and intelligence systems. The growing dependence of these critical infrastructures on the IT infrastructure means that the former cannot be secure if the latter is not.

Although current technical approaches address some of our immediate needs, they do not provide adequate computer and network security. Fundamentally different architectures and technologies are needed so that the IT infrastructure as a whole can become secure.

Historically, the Federal government has played a vital, irreplaceable role in providing support for fundamental, long-term IT R&D, generating technologies that gave rise to the multibillion-dollar IT industry. The PITAC's review of current Federally supported R&D in cyber security finds an imbalance, however, in the current cyber security R&D portfolio: most support is for short-term, defense-oriented research; there is relatively little support for fundamental research to address the larger security vulnerabilities of the civilian IT infrastructure, which supports defense systems as well. Therefore, PITAC urges changes in the Federal government's cyber security R&D portfolio to:

- Increase Federal support for fundamental research in civilian cyber security by $90 million annually at NSF and by substantial amounts at agencies such as DARPA and DHS to support work in 10 high-priority areas identified by PITAC.

- Intensify Federal efforts to promote recruitment and retention of cyber security researchers and students at research universities, with an aim of doubling this profession's numbers by the end of the decade.

- Provide increased support for the rapid transfer of Federally developed cutting-edge cyber security technologies to the private sector.

- Strengthen the coordination of the Interagency Working Group on Critical Information Infrastructure Protection and integrate it under the Networking and Information Technology Research and Development (NITRD) Program.

These actions will lead the way toward improving the Nation's cyber security, thereby promoting the security and prosperity of our citizens. We would be pleased to discuss this report with you and members of your Administration.

Sincerely,

Marc R. Benioff PITAC Co-Chair	Edward D. Lazowska PITAC Co-Chair

Appendix C

PITAC Executive Summary
(from February 2005 Report: *Cyber Security: A Crisis of Prioritization*)

The information technology (IT) infrastructure of the United States, which is now vital for communication, commerce, and control of our physical infrastructure, is highly vulnerable to terrorist and criminal attacks. The private sector has an important role in securing the Nation's IT infrastructure by deploying sound security products and adopting good security practices. But the Federal government also has a key role to play by supporting the discovery and development of cyber security technologies that underpin these products and practices. The PITAC finds that the Federal government needs to fundamentally improve its approach to cyber security to fulfill its responsibilities in this regard.

Background

The Nation's IT infrastructure has undergone a dramatic transformation over the last decade. Explosive growth in the use of networks to connect various IT systems has made it relatively easy to obtain information, to communicate, and to control these systems across great distances. Because of the tremendous productivity gains and new capabilities enabled by these networked systems, they have been incorporated into a vast number of civilian applications, including education, commerce, science and engineering, and entertainment. They have also been incorporated into virtually every sector of the Nation's critical infrastructure – including communications, utilities, finance, transportation, law enforcement, and defense. Indeed, these sectors are now critically reliant on the underlying IT infrastructure.

At the same time, this revolution in connectivity has also increased the potential of those who would do harm, giving them the capability to do so from afar while armed with only a computer and the knowledge needed to identify and exploit vulnerabilities. Today, it is possible for a malicious agent to penetrate millions of computers around the world in a matter of minutes, exploiting those machines to attack the Nation's critical infrastructure, penetrate sensitive systems, or steal valuable data. The growth in the number of attacks matches the tremendous growth in connectivity, and dealing with these attacks now costs the Nation billions of dollars annually. Moreover, we are rapidly losing ground to those who do harm, as is indicated by the steadily mounting numbers of compromised networks and resulting financial losses.

Beyond economic repercussions, the risks to our Nation's security are clear. In addition to the potential for attacks on critical targets within our borders, our national defense systems are at risk as well, because the military increasingly relies on ubiquitous communication and the networks that support it. The Global Information Grid (GIG), which is projected to cost as much as $100 billion and is intended to improve military communications by linking weapons, intelligence, and military personnel to each other, represents one such critical network. Since military networks interconnect with those in the civilian sector or use similar hardware or software, they are susceptible to any vulnerability in these other networks or technologies. Thus cyber security in the civilian and military sectors is intrinsically linked.

Although the large costs associated with cyber insecurity have only recently become manifest, the Nation's cyber security problems have been building for many years and will plague us for many years to come. They derive from a decades-long failure to develop the security protocols and practices needed to protect the Nation's IT infrastructure, and to adequately train and grow the numbers of experts needed to employ those mechanisms effectively. The short-term patches and fixes that are deployed today can be useful in response to isolated vulnerabilities, but they do not adequately address the core problems. Rather, fundamental, long-term research is required to develop entirely new approaches to cyber security. It is imperative that we take action before the situation worsens and the cost of inaction becomes even greater.

Tom Leighton

Co-Founder and Chief Scientist
Akamai Technologies, Inc.

Tom Leighton co-founded Akamai Technologies in September 1998. Serving as Chief Scientist, Dr. Leighton is Akamai's technology visionary as well as a key member of the Executive Committee setting the company's direction.

As one of the world's preeminent authorities on algorithms for network applications, Dr. Leighton's work behind establishing Akamai was based on recognizing that a solution to freeing up Web congestion could be found in applied mathematics and algorithms. Akamai has demonstrated this through the creation of the world's largest distributed computing platform that dynamically routes content and applications across a network of over 15,000 servers. Dr. Leighton's technology achievements at Akamai earned him recognition as one of the Top 10 Technology Innovators in U.S. News & World Report.

A Professor of Applied Mathematics at MIT, he has served as the Head of the Algorithms Group in MIT's Laboratory for Computer Science since its inception in 1996.

Dr. Leighton holds numerous patents involving cryptography, digital rights management, and algorithms for networks. During the course of his career, he has served on dozens of government, industrial, and academic review committees; program committees; and editorial boards. He is a former two-term chair of the 2,000-member Association of Computing Machinery Special Interest Group on Algorithms and Complexity Theory, and a former two-term editor-in-chief of the Journal of the ACM, the nation's premier journal for computer science research. Dr. Leighton is a Fellow for the American Academy of Arts and Sciences, and is currently serving as Chair of the President’s Information Technology Advisory Committee (PITAC) Subcommitte on Cyber Security. In 2004 he was elected into the National Academy of Engineering for contributions to the design of networks and circuits and for technology for Web content delivery.

Dr. Leighton has published more than 100 research papers, and his leading text on parallel algorithms and architectures has been translated into several languages. In 2002, Dr. Leighton was recognized by his alma mater as Princeton University's seventh Gordon Wu Distinguished Lecturer. He graduated summa cum laude from Princeton with a B.S. in Engineering. He received his Ph.D. in Mathematics from MIT.